Abstract

Cloud computing as one and all know is a computing area which has evolved from grid, utility computing, virtualization and SOA. As per the knowledge a cloud based infrastructure is based on certain elements like extended elasticity, metered service, on demand service availability, clustered resources and large network access. For providing these services or features it follows certain cloud service adoption models. All these models face some security concerns or the others. In the past many security models are presented by many researchers for resolving them and giving out a better known solution to IT industry adopting cloud. This paper aims at analyzing issues involved with virtualized architecture incurred while cloud
migration, figuring out various security measures from varying risk levels and present a refined or distinguished security model or solution based on all those issues discussed throughout the study. Main focus of the analysis carried here is on issues involved while adopting virtualization based infrastructure for moving in cloud, authentication based risks, risks incurred while data migration, attack on VM’s, issues while adopting virtualization, risk generated from malicious insiders are few to be discussed here.

References

- NIST, Guidelines on Security and Privacy in Public Cloud Computing, presented in 2011

Index Terms

Computer Science

Security
Keywords
Cloud Security Threats  Virtualization  VM (Virtual machine)  CSP (Cloud service provider)  Hypervisor  Virtual machine manager (VMM)  VDC (Virtualized data center)